

02
00n 4 10

a step of decoding data on said storage medium with the decoded
key data corresponding to the unit storage-area where the data have been read.

REMARKS

Attached hereto is a marked-up version of the changes made to the claims by the current amendment. The attached Appendix is captioned "**Version with Markings to Show Changes Made.**"

As a preliminary matter, Applicants again request acknowledgement of the JP '021 reference filed with an Information Disclosure Statement on October 20, 2000. A copy of the 1449 form filed with that IDS is attached.

Claim 7 stands rejected under 35 U.S.C. §112, first paragraph, as containing subject matter not described in the originally filed specification. Applicants respectfully traverse because claim 7 is supported by the fourth embodiment in the specification described in FIGS. 11-14. The fourth embodiment describes the use of a plurality of user passwords (Applicants' specification, page 19, lines 14-16). In particular, the specification specifically describes what is obtained by (1) encrypting the random number data with the user password PW1 and writing that to the region L1, and (2) encrypting the password PW1 with PW2 and writing that to the region L2 (Applicants' specification, page 19, line 22 to page 20, line 5). Moreover, the steps of obtaining the password

PW1 from L1 is described on page 21, lines 9-15. Accordingly, Applicants respectfully request that the §112, first paragraph, rejection of claim 7 be withdrawn.

Claims 18 and 19 stand rejected under 35 U.S.C. §112, second paragraph, as being indefinite. In response, Applicants amended claims 18 and 19 to more clearly recite the features of the present invention, without narrowing their scope. Accordingly, Applicants respectfully request that the §112, second paragraph, rejection of claims 18 and 19 be withdrawn.

Claim 15 stands rejected under 35 U.S.C. §101 for being directed to non-statutory subject matter. In response, Applicants amended claim 15 to more clearly recite the features of the present invention, without narrowing the scope of claim 15. Accordingly, Applicants respectfully request the §101 rejection of claim 15 be withdrawn.

Claims 1, 6-8 and 13-19 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Ganesan (U.S. Patent No. 5,748,735) in view of Kaufman (U.S. Patent No. 6,178,508). Applicants respectfully traverse because the cited references do not disclose or suggest features of "generating different key data for each of a plurality of unit storage areas of said storage medium" and "encrypting each said different key data for each unit storage area with said password," as recited in claim 1 and similarly recited in claims 8, 15, and 18. In addition, Applicants further respectfully traverse because the cited references do not disclose or suggest a step of decoding data on said storage medium with the

decoded key data corresponding to the unit storage area where the data have been read, as now recited in amended claim 19. Moreover, because the purposes and benefits of the cited references are different from the present invention, any optimization of the parameters of the cited references would be directed towards achieving them, and not to achieving the purposes and benefits of the present invention. Thus, even if, *arguendo*, the cited references, if combined, do disclose the features of the claims, there is, nevertheless, no motivation or suggestion to make the features of the claims, as recited.

One of the objects of the present invention is to protect data stored on a storage medium that is capable of changing key data with one password on a memory unit, such as a logic sector. In the present invention, data is encrypted by using a key data, which is generated separately (Applicants' specification, page 4, lines 13-15). The key data is encrypted with the password serving as a key, and written to the storage medium (Applicants' specification, page 4, lines 15-17). When in the reading process, the encrypted key data is decoded with the password to obtain the key data (Applicants' specification, page 4, lines 17-19). In turn, the data is then decoded using the decoded key data (Applicants' specification, page 4, line 19). Because the data is encrypted using key data that is generated separately from the password, the password cannot be deciphered by analyzing the cipher text (Applicants' specification, page 4, line 20-25). In addition, a different key data can be generated according to the specification of the memory unit, such as logic sectors (Applicants' specification, page 4, lines 20 to page 5, line 4). These

benefits are especially important for protecting data that are stored on removable disks (MO) or removable disk units (portable HDD).

In contrast, the purposes and benefits of the Ganesan reference relates to exchanges of symmetric session crypto-keys between users of virtual area networks, such as the Internet (Col. 5, lines 50-53). The cited reference relates to public-key cryptography, which is different from the present invention. First, the cited reference's protection of data generally involves multiple different computer servers that must be connected to the Internet, namely the security server (FIG. 2; Col. 6, lines 5-14). As a result, the cited reference's purpose relates to secure exchange of communication via an insecure network. Second, the private key data must be stored on a security server using the Yaksha database, which is essential to the security of the exchanged communication (FIG. 2). In contrast, in the present invention, different key data for each of the divided unit storage areas and the password are all stored on the storage medium. The only requirement is that a CPU be used to process the encryption and decoding of the information. Thus, no specific security server or Yaksha database is needed in the present invention. Accordingly, the Ganesan reference neither discloses or suggests the features of "generating different key data for each of a plurality of unit storage areas of said storage medium" and "encrypting each said different key data for each unit storage area with said password," as recited in claim 1 and similarly recited in claims 8, 15, and 18, nor does it disclose or suggest a step of decoding

data on said storage medium with the decoded key data corresponding to the unit storage area where the data have been read, as now recited in amended claim 19.

The Kaufman reference, on the other hand, teaches away from the present invention. In particular, the cited reference specifically teaches the use of an unencrypted header file, which stores the username and cryptographically hashed password (Col. 2, lines 27-31). According to the cited reference, because the cryptographically hashed passwords are never kept in an unprotected, or unhashed, state of memory, the passwords are not vulnerable to access by an unintended party. As far as Applicants can determine, the focus of the cited reference is to avoid encrypting and decoding information, because information stored in random access memory can be accessed by unintended users. Thus, the Kaufman reference teaches away from the use of key data, and similarly does not disclose or suggest features, as recited in claims 1, 8, 15, 18 and 19.

Since, as shown, the purpose of the cited references is different from the present invention, any optimization of the parameters of the cited references would be directed towards achieving the purposes and benefits of the cited references, and not to achieving the purposes and benefits of the present invention. The Examiner has not shown that in order to protect data stored on a storage medium that is capable of changing key data with one password on a memory unit, and one of ordinary skill in the art would have been motivated to modify the device of cited references to include features to generate different key data for each of a plurality of unit storage areas of a storage medium and encrypting the

different key data for each unit storage area with a password, as recited in claim 1 and similarly recited in claims 8, 15, and 18, or a step of decoding data on said storage medium with the decoded key data corresponding to the unit storage area where the data have been read, as now recited in amended claim 19. Thus, Applicants respectfully submit that there is no motivation or suggestion to make the features recited in claims 1, 8, 15, 18 and 19.

Since claims 2-7, 9-14, 16 and 17 depend upon either claims 1 or 8, they necessarily include all of the features of the independent claims plus other additional features. Thus, Applicants submit that the §103 rejection of claims 2-7, 9-14, 16 and 17 has also been overcome for the same reasons mentioned above to overcome the §103 rejection of independent claims 1 and 8. Applicants respectfully request that the §103(a) rejection of claims 2-7, 9-14, 16 and 17 be withdrawn.

For all of the above reasons, Applicant respectfully requests reconsideration and allowance of all pending claims. The Examiner should contact the undersigned attorney if an interview would expedite prosecution.

Respectfully submitted,
GREER, BURNS & CRAIN, LTD.

By


Grace Law

Registration No. 48,872

September 18, 2002
300 South Wacker Drive, Suite 2500
Chicago, Illinois 60606
Telephone: 312.360.0080
Customer No. 24978